

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN**

CHARLES TYER and CHRISTOPHER
HAUSER, individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

FLAGSTAR BANCORP, INC. and
FLAGSTAR BANK, FSB,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Charles Tyer and Christopher Hauser (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, upon personal knowledge of facts and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendants Flagstar Bancorp, Inc. and Flagstar Bank, FSB (together “Flagstar” or “Defendants”).

NATURE OF THE ACTION

1. Plaintiffs bring this class action individually and on behalf of all other individuals (“Class members”) who had their sensitive personal information—including names, phone numbers, addresses, Social Security numbers (SSN), and

bank account information (collectively, “Personal Information”)—disclosed to unauthorized third parties during a data breach compromising Flagstar’s third-party vendors’ (Accellion) legacy File Transfer Appliance software (the “Data Breach”).

2. Accellion made headlines in late 2020 and early 2021 following its December 23, 2020 disclosure to numerous clients that criminals breached Accellion’s client-submitted data via a vulnerability in its represented “secure” file transfer application.¹

3. Accellion is a software company that provides third-party file transfer services to clients. Accellion makes and sells a file transfer service product called the File Transfer Appliance (“FTA”). Accellion’s FTA is a 20-year-old, obsolete, “legacy product” that was “nearing end-of-life”² at the time of the Data Breach.

4. During the Data Breach, unauthorized persons gained access to Accellion’s clients’ files—including Flagstar’s—by exploiting multiple zero-day vulnerabilities in Accellion’s FTA platform.

¹ Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger*, GIZMODO (Feb. 11, 2021, 8:47 P.M.), <https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357>.

² ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>.

5. On March 5, 2021, Flagstar publicly confirmed that the Personal Information of certain customers was compromised in the Data Breach. In an official release posted to its website, Flagstar identified:

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform and that we are one of numerous Accellion clients who were impacted.³

6. On Flagstar's dedicated page to the Accellion breach, Flagstar indicates that it is in the process of notifying impacted individuals, and that Flagstar is "aware that those responsible for this incident are in some cases contacting Flagstar customers by e-mail and by telephone."⁴

7. Flagstar's release is clear that its bank customers (and perhaps others) are already experiencing the fallout of the Data Breach, as criminals are already attempting to contact breach victims in an attempt to defraud victims.

8. At the time of the Data Breach, Flagstar was a client of Accellion. Accellion's services to Flagstar, and the other customers, included the use of

³ FLAGSTAR BANK, *Accellion Incident Information Center*, <https://www.flagstar.com/customer-support/accellion-information-center.html> (last visited July 14, 2021).

⁴ *Id.*

Accellion's outdated and vulnerable FTA platform for large file transfers. Flagstar had a duty and responsibility to its customers to ensure that the FTA was suitable from a data security standpoint to protect its customers sensitive Personal Information. Flagstar has ample resources, and should have engaged in a rigorous third-party vendor risk management and vetting process with Accellion's FTA. It failed to do all of this, putting its customers at risk of fraud and identity theft. As a result, the Personal Information of Flagstar's customers has been accessed by and disclosed to criminals without authorization, who were able to exploit vulnerabilities in Accellion's FTA product.

9. Flagstar was well aware of the data security shortcomings in the FTA product. Nevertheless, it continued to use FTA, putting its customers at risk of being impacted by a breach.

10. Defendants' failures to ensure that the file transfer services and products used by Flagstar were adequately secure fell far short of their obligations and Plaintiffs and Class members' reasonable expectations for data privacy, jeopardized the security of Plaintiffs and Class members' Personal Information, and exposed Plaintiffs and Class members to fraud and identity theft or the serious risk of fraud and identity theft.

11. As a result of Defendants' conduct and the resulting Data Breach, Plaintiffs' and Class members' privacy has been invaded, their Personal

Information has been exfiltrated, exposed to, and is now in the hands of criminals, they have suffered fraud or identity theft or face a substantial risk of identity theft and fraud, they have suffered a privacy injury, they have lost hours of time dealing with the fallout of the Data Breach, and they have been otherwise injured. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

12. Plaintiff Charles Tyler is an adult citizen of the state of Texas and resides in Friendswood, Texas. Believing Flagstar would implement and maintain reasonable security and practices to protect customer Personal Information, Mr. Tyler provided Personal Information to Flagstar. Mr. Tyler routinely banks with Flagstar. On or about March 15, 2021, Flagstar sent Mr. Tyler, and Mr. Tyler received, a letter confirming that his Personal Information was impacted by the Data Breach. In the letter, Flagstar identified that the nature of the information involved includes his “Social Security Number, First Name, Last Name, Account Number, Address.” As a result of learning that he was impacted by the Data Breach, Mr. Tyler has spent at least 11 hours looking through and monitoring his accounts for fraud, setting up credit monitoring, and taking other measures in the fallout of the Data Breach to prevent fraud and identity theft.

13. Plaintiff Christopher Hauser is an adult citizen of the state of Utah and resides in Roy, Utah. Believing Flagstar would implement and maintain reasonable security and practices to protect customer Personal Information, Mr. Hauser provided Personal Information to Flagstar. Mr. Hauser provided his Personal Information in connection with home mortgage services obtained from Flagstar. On or about March 15, 2021, Flagstar sent Mr. Hauser, and Mr. Hauser received, a letter confirming that his Personal Information was impacted by the Data Breach. In the letter, Flagstar identified that the nature of the information involved includes his “Social Security Number, First Name, Last Name, Phone Number, Address.” As a result of learning that he was impacted by the Data Breach, Mr. Hauser has spent at least 8 hours looking through and monitoring his accounts for fraud, setting up credit monitoring, and taking other measures in the fallout of the Data Breach to prevent fraud and identity theft. Mr. Hauser attempted to obtain identity monitoring services from Kroll, the company hired by Flagstar to provide such services. However, Mr. Hauser could not get any assistance from Kroll or any of Kroll’s representatives. Mr. Hauser instead spent \$239.99 to obtain identity theft and credit monitoring services from another company.

14. Defendant Flagstar Bancorp, Inc. (NYSE: FBC) is a Michigan corporation with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098.

15. Defendant Flagstar Bank, FSB is a Michigan-based federally chartered stock savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars (\$5,000,000.00) and is a class action in which one or more Class members are citizens of states different from Defendants.

17. The Court has personal jurisdiction over Defendants because they are headquartered and a principal place of business in Michigan, conduct significant business in Michigan, and otherwise have sufficient minimum contacts with and intentionally avail themselves of the markets in Michigan.

18. Venue properly lies in this judicial district because, *inter alia*, Defendants have a principal place of business in this district; transact substantial business, have agents, and are otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Flagstar Knowingly Used and Retained Accellion's Unsecure FTA Product

19. Accellion is a Palo Alto-based software company that makes, markets, and sells file transfer products and services.

20. Accellion's FTA product, which Flagstar and many of Accellion's other clients used, was known to be not secure and, by Accellion's own acknowledgment, outdated.

21. The FTA—or File Transfer Appliance—is Accellion's twenty-year-old “legacy” file transfer software, which purportedly is designed and sold for large file transfers.⁵

22. Accellion's FTA is an obsolete “legacy product” that was “nearing end-of-life,”⁶ thus leaving it vulnerable to compromise and security incidents. Accellion acknowledged that the FTA program is insufficient to keep file transfer processes secure “in today's breach-filled, over-regulated world” where “you need even broad

⁵ ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021), <https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/>.

⁶ ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>.

protection and control.”⁷ On the page dedicated to Accellion FTA, Accellion’s website states: “End-of-Life Announced for FTA. No Renewals After April 30, 2021.”⁸

23. Key people within Accellion had even acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion’s Chief Marketing Officer Joel York confirmed that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: “It just wasn’t designed for these types of threats”⁹

24. Accellion’s Chief Information Security Officer Frank Balonis stated: “Future exploits of [FTA] . . . are a constant threat. *We have encouraged all FTA customers to migrate to kiteworks for the last three years* and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting

⁷ ACCELLION, *Accellion FTA*, <https://www.accellion.com/products/fta/> (last visited July 15, 2021).

⁸ *Id.*

⁹ Jim Brunner & Paul Roberts, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington State Auditor*, SEATTLE TIMES (Feb. 3, 2021, 4:57 P.M.), <https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/>.

our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible.” (Emphasis added).¹⁰

25. Despite knowing that FTA left Flagstar and third parties interacting and transacting with its customers (like Plaintiffs and Class members) exposed to security threats, Flagstar continued to utilize, the FTA file transfer product at the time of the Data Breach.

C. The FTA Data Breach

26. On December 23, 2020, the inevitable happened: Accellion confirmed to numerous clients that it experienced a massive security breach whereby criminals were able to gain access to sensitive client data via a vulnerability in its FTA platform.¹¹

27. According to reports, including the security assessment report conducted by Accellion’s retained vendor Mandiant,¹² the criminals exploited as many as four zero-day vulnerabilities in a two-stage attack on Accellion’s FTA to steal sensitive data files associated with numerous of Accellion’s clients, which

¹⁰ ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>.

¹¹ Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger*, GIZMODO (Feb. 11, 2021, 8:47 P.M.), <https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357>.

¹² See <https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf> (last visited July 15, 2021).

include corporations, law firms, banks, healthcare service providers, universities, and other entities.

28. With respect to how Accellion's FTA was compromised, one report summarizes:

The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.¹³

29. The criminals, reportedly associated with the well-known Clop ransomware gang, the FIN11 threat group, and potentially other threat actors, launched the attacks in mid-December 2020. The attacks continued from at least mid-December 2020 and into January 2021, as these actors continued to exploit vulnerabilities in the FTA platform. Following the attacks, the criminals resorted to extortion, threatening Accellion's clients, e.g., by email, with making the stolen information publicly available unless ransoms were paid.¹⁴ In at least a few

¹³ Jai Vljayan, DARKReading, *Accellion Data Breach Resulted in Extortion Attempts Against Multiple Victims* (Feb. 22, 2021, 4:50 P.M.), <https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226>.

¹⁴ Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang*, BLEEPINGCOMPUTER (Feb. 22, 2021, 9:06 A.M.),

instances, the criminals carried these treats and published private and confidential information online. *See id.*

30. An example of a message sent by the criminals to a client of Accellion that was victimized during the breach is below¹⁵:

Hello!

Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address [http://\[redacted\].onion/](http://[redacted].onion/) - use TOR browser or [http://\[redacted\].onion.dog/](http://[redacted].onion.dog/) - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

31. Accellion has remained in the headlines through early 2021 (and continues to receive a raft of negative publicity) following its mid-December 2020 disclosure of the massive Data Breach. The list of groups and clients who used Accellion's unsecure FTA product and were impacted by the Data Breach continues to increase.

32. The list, to date, reportedly includes (but is not limited to):

- Allens
- American Bureau of Shipping ("ABS")
- Arizona Complete Health

<https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/>.

¹⁵ *Id.*

- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Health Net LLC (and related entities owned by Centene Corp.)
- Jones Day
- The Kroger Co.
- Morgan Stanley (StockPlan Connect)
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys
- The Reserve Bank of New Zealand
- Shell Oil Company
- Singtel
- Southern Illinois University School of Medicine
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- The University of Colorado
- The University of Miami

C. Flagstar Announces It Suffered a Data Breach

33. Flagstar Bank is a United States Midwest-based bank headquartered in Troy, Michigan. Flagstar has numerous branch and home loan center locations across the United States, and is one of the largest residential mortgage servicers in the country.

34. Per its website, Flagstar operates 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio, and its mortgage divisions operates nationally through 103 retail locations. With assets of \$31 billion, Flagstar touts that it is the sixth largest bank mortgage originator nationally, and the second largest savings bank in the country.¹⁶

35. On March 5, 2021, Flagstar publicly confirmed that the Personal Information of Flagstar customers was compromised in the Data Breach, by releasing a statement on its website.

36. On its webpage dedicated to the Accellion breach, Flagstar provides scant details regarding the Data Breach, including following information, in pertinent part¹⁷:

¹⁶ FLAGSTAR BANK, *About Flagstar*, <https://www.flagstar.com/about-flagstar.html> (last visited July 14, 2021).

¹⁷ FLAGSTAR BANK, *Accellion Incident Information Center*, <https://www.flagstar.com/customer-support/accellion-information-center.html> (last visited July 14, 2021).

Flagstar Bank Statement on Accellion Vulnerability

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform and that we are one of numerous Accellion clients who were impacted.

37. Flagstar also cautions its customers¹⁸:

Information Security Best Practices

We are aware that those responsible for this incident are in some cases contacting Flagstar customers by e-mail and by telephone. These are communications from unauthorized individuals responsible for the Accellion incident, and you should not respond to them. If you receive a suspicious message, please do not open attachments or click on links.

38. Flagstar's submissions to California's Attorney General¹⁹ provides little additional information regarding the nature of the data impacted in the breach, and is very similar to its dedicated webpage for the Data Breach. The incident reportedly did not affect Flagstar's IT infrastructure outside of the Accellion platform, and Flagstar claims that it has permanently discontinued the use of Accellion's FTA.²⁰

¹⁸ *Id.*

¹⁹ CALIFORNIA ATTORNEY GENERAL, *Submitted Breach Notification Sample*, <https://oag.ca.gov/system/files/Flagstar%20Bank%20Ad%20Standard%20r3prf.pdf> (last visited Apr. 21, 2021).

²⁰ *Id.*

39. Flagstar's public statements and notification letter state that it is working to notify and impacted customers, and that Flagstar has secured the services of Kroll to provide identity monitoring for impacted persons for two years.²¹

40. According to reports, screenshots of stolen Flagstar records and information suggest that impacted data includes sensitive information, including SSN, names, addresses, phone numbers, and tax records.²²

D. Impact of the Data Breach

41. The actual extent and scope of the impact of the Data Breach on Flagstar's customers remains uncertain.

42. Flagstar has confirmed that it has stopped using Accellion's jeopardized FTA services, but unfortunately for Plaintiffs and Class members, the damage is already done.

43. Flagstar had an obligation and duty to its customers to protect the sensitive Personal Information it collected and required for collection as part of doing business with Flagstar. It also had a duty to ensure that any third parties to which Flagstar entrusted customers' sensitive Personal Information were well-

²¹ *Id.*

²² Dora Tudor, *US Bank and Mortgage Lender Flagstar Victim of a major data breach*, HEIMDAL SECURITY (Mar. 9, 2021), <https://heimdalsecurity.com/blog/flagstar-bank-major-data-breach/>.

vetted and capable of keeping sensitive information safe and out of the hands of criminals. With assets of \$31 billion, as the sixth largest bank mortgage originator nationally and second largest savings bank in the country, Flagstar had vast resources to develop and maintain a robust third-party vendor risk management program to vet its vendors like Accellion, and ensure that the vendors it engages with are adequate and will not jeopardize the security of its customers' sensitive information. Flagstar is heavily regulated as a financial institution, and it knew of the importance of maintaining the privacy and safeguarding sensitive financial information of its customers. Flagstar utterly failed in carrying these duties and responsibilities, and placed its customers' Personal Information in the hands of a vendor, Accellion, that it knew or should have known would jeopardize the security of that sensitive information.

44. Flagstar has known that the FTA software is unsecured and should no longer be used in connection with data transfers. Indeed, “[m]ultiple cybersecurity experts . . . highlight that Accellion FTA is a 20-year-old application designed to allow an enterprise to securely transfer large files but it is nearing the end of life,” and that “Accellion asked its customers late last year to switch over to a new product it offers called kiteworks.”²³ Flagstar failed to promptly make the switch to

²³ Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021, 6:17 A.M.),

Kiteworks or some other secure file transfer solution, and it knowingly continued to use FTA, exposing Class members' Personal Information to potential theft, identity theft, and fraud.

45. The harm caused to Plaintiffs and Class members by the Data Breach is already apparent. As identified herein, criminal hacker groups already are threatening Accellion's clients with demands for ransom payments to prevent sensitive Personal Information from being disseminated publicly.

46. Even if companies, like Flagstar, that were impacted by the Accellion Data Breach pay these ransoms, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive Personal Information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

47. The Data Breach was particularly damaging given the nature of Accellion's FTA. In the words of one industry expert: "[The] vulnerabilities [in Accellion's FTA] are particularly damaging, because in a normal case an attacker has to hunt to find your sensitive files, and it's a bit of a guessing game, but in this

<https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/>.

case the work is already done . . . By definition everything sent through Accellion was pre-identified as sensitive by a user.”²⁴

48. The Data Breach creates a heightened security concern for Plaintiffs and Class members because SSNs and other banking and tax information was potentially disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

49. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers “can be an identity thief’s most valuable piece of consumer information.”²⁵

²⁴ Lily Hay Newman, *The Accellion Breach Keeps Getting Worse—and More Expensive*, WIRED.COM (Mar. 8, 2021, 7:00 A.M.), <https://www.wired.com/story/accellion-breach-victims-extortion> (quoting Jake Williams, founder of the security firm Rendition Infosec).

²⁵ *Fact Sheet: The Work of the President’s Identity Theft Task Force*, DEP’T OF JUSTICE (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

50. Flagstar had a duty to keep Plaintiffs' and Class members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class members provided their Personal Information to Flagstar with the understanding that Flagstar and any business partners to whom Flagstar disclosed the Personal Information (i.e., Accellion) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

51. Defendants' data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in Accellion's industry of data collection and transfer.

52. Data breaches, including third-party vendor breaches, are by no means new and they should not be unexpected. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

53. It is well known amongst companies that collect, maintain, and store sensitive personally identifying information that the sensitive information—like the SSNs—is valuable and frequently targeted by criminals. In a recent article, one

commentator noted that “[d]ata breaches are on the rise for all kinds of businesses Many of them were caused by flaws in . . . systems either online or in stores.”²⁶

54. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

55. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁷

56. With access to an individual’s Personal Information, criminals can do more than just empty a victim’s bank account—they can also commit all manner of fraud, including: obtaining a driver’s license or official identification card in the

²⁶ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 11:05 A.M.), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

²⁷ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GOVINFO.GOV, June 4, 2007, <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (emphasis added).

victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.²⁸

57. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other Personal Information directly on various illegal websites making the information publicly available, often for a price.

58. A recent study concluded that the value of information available on the dark web sufficient to commit identity theft or fraud is about \$1,010 per identity. The study identified that "[a] full range of documents and account details allowing identity theft can be obtained for \$1,010."²⁹ Data breaches and identity theft have a

²⁸ See FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited Apr. 21, 2021).

²⁹ CISON, *You Are Worth \$1,010 on the Dark Web, New Study by PrivacyAffairs Finds* (Mar. 8, 2021, 5:15 ET), <https://www.prnewswire.com/news-releases/you->

crippling effect on individuals and detrimentally impact the entire economy as a whole.

59. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Flagstar failed to take reasonable steps to vet Accellion's FTA product, to protect its customers' sensitive Personal Information from being breached and exposed to criminals; and to migrate away from the unsecure FTA platform, instead leaving Class members exposed to risk of fraud and identity theft.

60. Flagstar is, and at all relevant times has been, aware that the sensitive Personal Information it collects, handles, stores, and shares with third parties in connection with file transfer processes is highly sensitive. As a heavily regulated financial institution, Flagstar is aware of the importance of safeguarding that information and protecting its systems and customers from security vulnerabilities.

61. Flagstar was aware, or should have been aware, of regulatory and industry guidance regarding data security, and Flagstar was alerted to the risk associated with failing to ensure that the FTA product it was using for file transfers was adequately secured or failing to switch to a more secure file transfer solution.

are-worth-1-010-on-the-dark-web-new-study-by-privacyaffairs-finds-301241816.html.

62. Despite the well-known risks of hackers and cybersecurity intrusions, Flagstar failed to employ adequate data security measures in connection with its use of Accellion's FTA platform in a meaningful way in order to prevent a breach of its customers' Personal Information.

63. Flagstar's failure adequately to vet and audit Accellion's FTA product and related services, and its continued use of the legacy, outdated, and usecured product, run afoul of industry best practices and standards.

64. Despite the fact that Flagstar was on notice of the very real possibility of data theft associated with the FTA platform, it still failed to make necessary changes and permitted a massive intrusion to occur that resulted in disclosure of Plaintiffs' and Class members' Personal Information to criminals.

65. Defendants permitted Class members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

66. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has

identified that: “If your data was stolen through a data breach that means you were somewhere out of compliance” with payment industry data security standards.³⁰

67. As a result of the events detailed herein, Plaintiffs and Class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

68. As a result of the Data Breach, Plaintiffs’ and Class members’ privacy has been invaded, their Personal Information is now in the hands of criminals, they have suffered concrete data breach injury, they face a substantially increased risk of identity theft and fraud, and they have taken and must continue to take time-consuming action to protect themselves from such identity theft and fraud.

³⁰ Lisa Baertlein, *Flagstar Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), <http://www.reuters.com/article/us-Flagstar-cyber-idUSKBN18M2BY>.

CLASS ALLEGATIONS

69. Plaintiffs bring this action on behalf of herself and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

Nationwide Class

All persons in the United States to whom Flagstar sent breach notification letters confirming that their Personal Information was compromised in the Data Breach.

Texas Class

All persons in Texas to whom Flagstar sent breach notification letters confirming that their Personal Information was compromised in the Data Breach.

Utah Class

All persons in Utah to whom Flagstar sent breach notification letters confirming that their Personal Information was compromised in the Data Breach.

70. Excluded from the Classes are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

71. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appears to include hundreds of thousands or millions of members who are geographically dispersed.

72. **Typicality**: Plaintiffs' claims are typical of Class members' claims. Plaintiffs and all Class members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class members

they seek to represent. Accordingly, Plaintiffs' claims are typical of Class members' claims.

73. **Adequacy**: Plaintiffs' interests are aligned with the Classes they seek to represent, and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and undersigned counsel intend to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiffs and undersigned counsel.

74. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class member's claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

75. **Commonality and Predominance**: The following questions common to all Class members predominate over any potential questions affecting individual Class members:

- whether Flagstar engaged in the wrongful conduct alleged herein;
- whether Flagstar had a duty to protect Personal Information, and whether it breached that duty;
- whether Flagstar had a duty to, but failed to, vet and audit its third party file transfer vendor, Accellion;
- whether Flagstar's data security practices resulted in the disclosure of Plaintiffs' and other Class members' Personal Information;
- whether Flagstar knew or should have known of the unsecure nature of the FTA file transfer product, but continued to use the product;
- whether Flagstar's conduct was negligent or negligent *per se*;
- whether Flagstar formed implied contracts with Plaintiffs and Class members and, if so, whether data security and privacy was a term of those implied contracts;
- whether Flagstar breached implied contracts with Plaintiffs and Class members;

- whether Flagstar violated consumer data privacy statutes;
- whether Defendants violated privacy rights and invaded Plaintiffs' and Class members' privacy; and
- whether Plaintiffs and Class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

76. Given that Flagstar engaged in a common course of conduct as to Plaintiffs and the Classes, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I Negligence

77. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

78. Flagstar inadequately vetted Accellion and its FTA product, and continued using the product which Accellion acknowledged is vulnerable to security breaches, and which was a legacy, end-of-life product.

79. Flagstar collected, was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiffs and Class members, including sensitive banking information and Social Security numbers, among other information.

80. Flagstar knew, or should have known, of the risks inherent to storing

the Personal Information of Plaintiffs and Class members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Flagstar, because Accellion had previously recognized and acknowledged the data security concerns with its FTA product.

81. Flagstar owed a duty of care to Plaintiffs and Class members whose Personal Information had been entrusted to it. Flagstar's duty included obligations such as auditing and testing the FTA periodically, through penetration testing or otherwise, using updated and secured file transfer solutions, and taking other measures to ensure the protection and safeguarding of Personal Information.

82. Flagstar breached its duties to Plaintiffs and Class members by failing to do all of the foregoing and failing provide fair, reasonable, or adequate data security in connection transacting business with its customers.

83. Flagstar's duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that Flagstar is intended to, and represents that it will, handle securely. Indeed, on its website, Flagstar represents that it "is committed to maintaining the security of the data you provide us." This duty includes a rigorous and adequate process for vetting third-party vendors to which Flagstar entrusts sensitive Personal Information of its customers.

84. Flagstar's duty of care also arises from the statutory framework of laws including Section 5 of the FTC Act, the Gramm-Leach-Bliley Act, and the CCPA,

all of which required Flagstar to properly and securely handle and maintain sensitive customer Personal Information, and all of which Flagstar violated as discussed *infra*.

85. Flagstar also had a duty to promptly and timely notify Plaintiffs and Class members of the Data Breach in order to prevent additional harm, but failed to do so. Instead, Flagstar unreasonably delayed in notifying impacted persons of the breach, causing harm due to the delay that was foreseeable, including preventing Plaintiffs and Class members from promptly protecting themselves in response to the Data Breach.

86. But for Flagstar's wrongful and negligent breach of duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

87. There is substantial nexus between Flagstar's alleged misconduct and the injuries suffered by Plaintiffs and Class members. Plaintiffs and Class members were the foreseeable victims of Flagstar's misconduct and data security failures, and their harm was the natural and foreseeable consequence of such misconduct and failures, and Flagstar's breaches of duties owed. Flagstar acted with wanton disregard for the security of Plaintiffs' and Class members' Personal Information, especially in light of the fact that for years Accellion warned of the data security concerns relating to the FTA, and in light of Flagstar's knowledge that sensitive

Personal Information is attractive and valuable to criminals.

88. A “special relationship” exists between Flagstar, on the one hand, and Plaintiffs and Class members, on the other hand. Flagstar entered into a “special relationship” with Plaintiffs and Class members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiffs and Class members.

89. As a direct and proximate result of Flagstar’s negligent conduct, Plaintiffs and Class members have suffered concrete injury, face an increased risk of future harm, and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence Per Se

90. Plaintiffs reallege and incorporates all previous allegations as though fully set forth herein.

91. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), and the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801, *et seq.* (“GLBA”), among other statutes, Flagstar had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs’ and Class members’ Personal Information.

92. Flagstar breached its duties to Plaintiffs and Class members under the Federal Trade Commission Act (15 U.S.C. § 45), and the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801, *et seq.* (“GLBA”), among other statutes, by failing to provide

fair, reasonable, or adequate data security in connection with the use of the FTA platform in order to safeguard Plaintiffs' and Class members' Personal Information.

93. Specifically, the GLBA states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a). The GLBA gave rise to, and Flagstar had, a duty of reasonable care to protect Plaintiffs' and Class members' Personal Information. Flagstar fell short in that duty, in violation of the GLBA. Flagstar violated the GLBA and related regulations by failing to secure customers' Personal Information from exposure to unauthorized third parties, by failing to identify foreseeable risks to the security of its customers' data and maintain protocols to control those risks, and by failing to select and retain a third-party file transfer vendor capable of maintaining appropriate safeguards for its customers' information.

94. Flagstar's failure to comply with applicable laws and regulations constitutes negligence per se.

95. But for Flagstar's wrongful and negligent breach of duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

96. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Flagstar knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Personal Information.

97. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have been harmed or now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Contract

98. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

99. Flagstar provides banking and mortgage services to Plaintiffs and Class members. In connection with banking with Flagstar, Plaintiffs and Class members entered into implied contracts with Flagstar.

100. Pursuant to these implied contracts, Plaintiffs and Class members provided Flagstar with their Personal Information, which was required by Flagstar. In exchange, Flagstar agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and

Class members' Personal Information, including ensuring that third parties to which Flagstar provided Personal Information would also keep the information secure; and (2) to protect Plaintiffs' and Class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

101. The protection of Personal Information was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Flagstar, on the other hand. Had Plaintiffs and Class members known that Flagstar would not adequately protect its customers' Personal Information they would not have done business with Flagstar and would not have provided Flagstar with their sensitive Personal Information.

102. Plaintiffs and Class members performed their obligations under the implied contract when they provided Flagstar with their Personal Information and used Flagstar's banking services.

103. Necessarily implicit in the agreements between Plaintiffs/Class members and Flagstar was Flagstar's obligation to take reasonable steps to secure and safeguard Plaintiffs' and Class members' Personal Information.

104. Flagstar breached its obligations under its implied contracts with Plaintiffs and Class members by failing to implement and maintain reasonable

security measures—including the use of inadequate third-party vendor Accellion—to protect their Personal Information.

105. Flagstar’s breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the exposure of their Personal Information.

106. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of Flagstar’s material breaches of its agreements.

107. Plaintiffs and other Class members were damaged by Flagstar’s breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT V
Invasion of Privacy

108. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

109. Plaintiffs and Class members had a reasonable expectation of privacy in the Personal Information that Flagstar disclosed without authorization.

110. By failing to keep Plaintiffs' and Class members' Personal Information safe, knowingly utilizing the unsecure FTA platform, and disclosing Personal Information to unauthorized parties for unauthorized use, Flagstar unlawfully invaded Plaintiffs' and Class members' privacy by, *inter alia*:

- a. intruding into Plaintiffs' and Class members' private affairs in a manner that would be highly offensive to a reasonable person; and
- b. invading Plaintiffs' and Class members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized third parties;
- c. failing to adequately secure their Personal Information from disclosure to unauthorized persons;
- d. enabling the disclosure of Plaintiffs' and Class members' Personal Information without consent.

111. Flagstar knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class members' position would consider its

actions highly offensive.

112. Flagstar knew or through reasonable diligence could have learned and should have known, that Accellion's FTA platform was vulnerable to data breaches.

113. Flagstar invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

114. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Flagstar's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

115. In failing to protect Plaintiffs' and Class members' Personal Information, and in disclosing Plaintiffs' and Class members' Personal Information, Defendants acted with malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private.

116. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT VI
Violations of the Michigan Consumer Protection Act,
Mich. Comp. Laws Ann. § 445.901, *et seq.*

117. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

118. Plaintiffs are “persons” are defined by Mich. Comp. Laws Ann. § 445.903(d).

119. Flagstar advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. 445.903(g).

120. Flagstar engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb);

d. Failing to reveal facts that are material to the transaction in light of representation of fact made in a positive manner, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

121. Flagstar's unfair, unconscionable, and deceptive practices include, among other things:

- a. failing to implement and maintain reasonable security measures—including the use of inadequate third-party vendor Accellion—to protect their Personal Information;
- b. failing to identify foreseeable risks to the security of its customers' data and maintain protocols to control those risks, and by failing to select and retain a third-party file transfer vendor capable of maintaining appropriate safeguards for its customers' information;
- c. failing to develop and maintain a robust third-party vendor risk management program to vet its vendors like Accellion, and failing to ensure that the vendors it engages with are adequate and will not jeopardize the security of its customers' sensitive information;
- d. failing to utilize, and omitting, suppressing, or concealing the material fact that it does not utilize, industry standard security

practices but, instead, utilize the unsecured FTA platform and did not properly vet its vendor Accellion.

122. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its security procedures and practices and ability to protect its customers' Personal Information.

123. By failing to disclose that it does not enlist industry standard security practices, fails to adequately vet third-party vendors providing file transfer solutions that are entrusted with Personal Information, and utilized the unsecured FTA platform despite it being a legacy product that was known to be vulnerable, all of which rendered Class members particularly vulnerable to data breaches, Flagstar engaged in unfair, unconscionable, and deceptive practices, in violation of Mich. Comp. Laws Ann. § 445.903.

124. A reasonable consumer would not have banked or sought mortgage and financial services (or remained as customers) with Flagstar if they knew the truth about its security procedures and that it used a third-party vendor, i.e., Accellion, for file transfers that utilize unsecured transfer applications. By withholding material information about its security practices, Flagstar was able to obtain customers who provided and entrusted their Personal Information in connection with doing business with Flagstar. Had Plaintiffs known the truth about Flagstar's

security procedures and that it does business with Accellion using Accellion's unsecured FTA, Plaintiffs would not have done business with Flagstar.

125. As a result of Defendants' violations of Michigan's Consumer Protection Act, Plaintiffs and Class members are entitled to injunctive or other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including, but not limited to: (1) ordering that Flagstar end the use of the FTA platform; (2) ordering that Defendants utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (3) ordering that Flagstar, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems and third-party software on a periodic basis; (4) ordering that Defendants engage third party security auditors and internal personnel, and develop or enhance a third-party vendor risk management program, consistent with industry standard practices; (5) ordering that Defendants audit, test and train its security personnel regarding data security in the context of third-party vendors and file transfer processes, including any new or modified procedures; (6) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions

of those systems; (7) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (8) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendants, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive Personal Information for vulnerabilities to prevent threats to customers; (10) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (11) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Defendants' customers must take to protect themselves; and (12) ordering Flagstar to engage in "dark web" monitoring for a period of no less than 5 years to continue to monitor for fraudulent use or activity concerning Class members' Personal Information.

126. As a result of Flagstar's violations of Michigan's Consumer Protection Act, Plaintiffs and Class members have suffered injury in fact and lost money or property, as detailed herein. They agreed to bank with Flagstar, or made purchases or spent money that they otherwise would not have made or spent, had they known

the truth. Class members lost Personal Information, which is their property. Class members lost money as a result of dealing with the fallout of the Data Breach, including, among other things, negative credit reports, the value of time they expended monitoring their credit and transactions, resolving fraudulent charges, and resolving issues that resulted from the fraudulent charges and replacement of cards.

127. Plaintiffs request that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Flagstar not engaged in the foregoing violations, including by ordering restitution of all funds that Flagstar may have acquired from Plaintiffs and Class members as a result of those violations.

COUNT VII Unjust Enrichment

128. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

129. Flagstar has profited and benefited from the monies or fees paid by Plaintiffs and Class members to receive services from Flagstar.

130. Flagstar has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiffs and Class members did not receive services of the

quality, nature, fitness, or value represented by Flagstar and that reasonable consumers expected.

131. Flagstar has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiffs and Class members.

132. Equity and justice militate against permitting Flagstar to retain these profits and benefits.

133. Plaintiffs and Class members suffered injury as a direct and proximate result of Flagstar's unjust enrichment and seek an order directing Flagstar to disgorge these benefits and pay restitution to Plaintiffs and Class members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representatives and undersigned counsel as class counsel;

B. Award Plaintiffs and Class members actual and statutory damages to the maximum extent allowable;

D. Award Plaintiffs and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 15, 2021

Respectfully submitted,

/s/ Nicholas A. Coulson

Nicholas a. Coulson
ncoulson@ldclassaction.com

LIDDLE & DUBIN, P.C.

975 E. Jefferson Ave.
Detroit, Michigan 48207
Telephone: 313.392.0015
Facsimile: 313.392.0025

Tina Wolfson (*pro hac vice* to be filed)

twolfson@ahdootwolfson.com

Robert Ahdoot (*pro hac vice* to be filed)

rahdoot@ahdootwolfson.com

Theodore Maya (*pro hac vice* to be filed)

tmaya@ahdootwolfson.com

AHDOOT & WOLFSON, PC

2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Andrew W. Ferich (*pro hac vice* to be filed)

aferich@ahdootwolfson.com

AHDOOT & WOLFSON, PC

201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

Counsel for Plaintiffs